PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-307043
(43)Date of publication of application : 02.11.2001

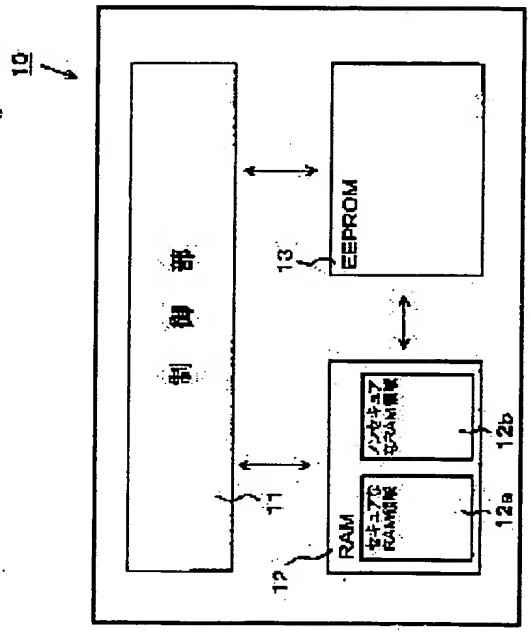
(51)Int.CI. G06K 19/07
G06F 9/06
G06F 12/14
G06K 19/073

(21)Application number : 2000-117323
(22)Date of filing : 19.04.2000

(71)Applicant : DAINIPPON PRINTING CO LTD
(72)Inventor : NOZAWA AKIO
KUNIMOTO SATOHARU
CHIKADA YASUYUKI

(54) MULTI-APPLICATION IC CARD AND ITS PROCESSING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a multi-application IC card with high security capable of shortening the processing time, and its processing method.
SOLUTION: This multi-application IC card is provided with a storage means 12 including a secured area 12a access to which is made impossible from the application after switching by resetting information application before the switching when plural applications are switched to be executed. It is provided with a confirming means 11 for confirming whether or not the security of the first application is satisfied, a setting means 12 for setting a security status in the secured area when the security is satisfied, a saving means 13 for saving the security status at switching from the first to the second application and a decoding means for decoding the saved security status at switching from the second to the first application.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－307043
（P2001－307043A）
(43)公開日　平成13年11月２日(2001.11.2)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　19/07		Ｇ０６Ｆ　9/06	５５０Ａ	５Ｂ０１７
Ｇ０６Ｆ　9/06	５５０		３１０Ｊ	５Ｂ０３５
12/14	３１０	Ｇ０６Ｋ　19/00	Ｎ	５Ｂ０７６
Ｇ０６Ｋ　19/073			Ｐ	

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

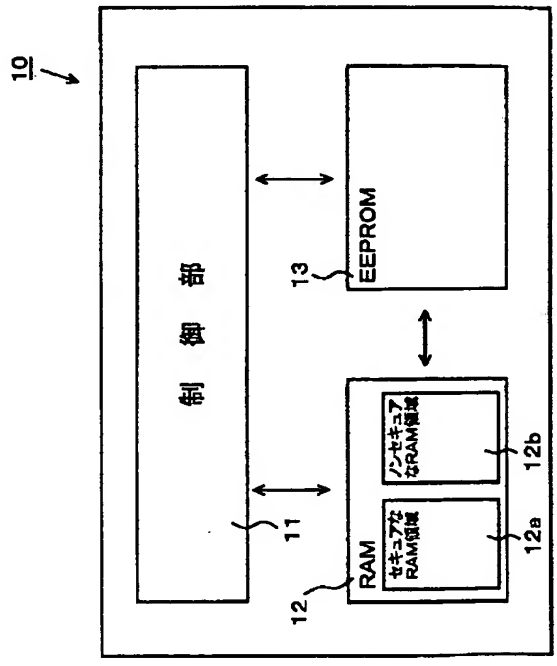
(21)出願番号　特願2000－117323(P2000－117323)
(22)出願日　平成12年４月19日(2000.4.19)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　野澤　昭雄
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(72)発明者　國本　聡治
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(74)代理人　100092576
弁理士　鎌田　久男

最終頁に続く

(54)【発明の名称】　マルチアプリケーションＩＣカード及びその処理方法

(57)【要約】
【課題】　処理時間を短縮することができ、セキュリティ性の高いマルチアプリケーションＩＣカード及びその処理方法を提供する。
【解決手段】　切り替えて実行する複数のアプリケーションの切替時に切替前のアプリケーションの情報をリセットして切替後のアプリケーションからはアクセス不能なセキュアな領域１２ａを含む記憶手段１２を有するマルチアプリケーションＩＣカードであって、第１のアプリケーションのセキュリティが満足できるか否かを確認する確認手段１１と、セキュリティが満足できるときに、セキュリティステータスをセキュアな領域に設定する設定手段１２と、第１から第２のアプリケーションへの切替時に、セキュリティステータスを退避させる退避手段１３と、第２から第１のアプリケーションへの切替時に、退避したセキュリティステータスを復号させる復号化手段１２とを備える。



1

【特許請求の範囲】

【請求項１】　切り替えて実行する複数のアプリケーションを有し、アプリケーション切替時に切替前のアプリケーションの情報をリセットして切替後のアプリケーションからはアクセス不能なセキュアな領域を含む記憶手段を有するマルチアプリケーションＩＣカードであって、

第１のアプリケーションのセキュリティが満足できるか否かを確認するセキュリティ確認手段と、

セキュリティが満足できるときに、セキュリティステータスを、前記セキュアな領域に設定するセキュリティステータス設定手段と、

前記第１のアプリケーションから第２のアプリケーションへの切替時に、前記セキュアな領域に設定されたセキュリティステータスを退避させるセキュリティステータス退避手段と、

前記第２のアプリケーションから前記第１のアプリケーションへの切替時に、前記セキュリティステータス退避手段に退避させられたセキュリティステータスを前記セキュアな領域に復号させるセキュリティステータス復号化手段とを備えるマルチアプリケーションＩＣカード。

【請求項２】　請求項１に記載のマルチアプリケーションＩＣカードにおいて、

前記記憶手段は、アプリケーション切替後も切替前の記憶を保持し、切替後のアプリケーションからもアクセス可能なノンセキュアな領域を含み、

前記セキュリティステータス退避手段に退避させられたセキュリティステータスの復号を許可するための暗号情報を作成して前記ノンセキュアな領域に保存する暗号保存手段と、

前記第１のアプリケーションから前記第２のアプリケーションに切り替えた後、再度、前記第１のアプリケーションに切り替えたときに、再度、暗号情報を作成し、その作成した暗号情報と、前記ノンセキュアな領域に保存されている暗号情報とを比較する暗号比較手段とを備え、

前記セキュリティステータス復号化手段は、前記暗号比較手段で比較した暗号情報が一致する場合に、前記退避させたセキュリティステータスを復号させることを特徴とするマルチアプリケーションＩＣカード。

【請求項３】　請求項２に記載のマルチアプリケーションＩＣカードにおいて、

前記暗号保存手段は、初めに、暗号を作成し、その作成した暗号を暗号化キーとして保存し、次に、その暗号化キーに基づいて暗号情報を作成し、

前記暗号比較手段は、前記暗号化キーに基づいて暗号情報を作成することを特徴とするマルチアプリケーションＩＣカード。

【請求項４】　切り替えて実行する複数のアプリケーションを有し、アプリケーション切替時に切替前のアプリケーションの情報をリセットして切替後のアプリケーションからはアクセス不能なセキュアな領域及びアプリケーション切替後も切替前の記憶を保持し、切替後のアプリケーションからもアクセス可能なノンセキュアな領域を含む記憶手段を有するマルチアプリケーションＩＣカードの処理方法であって、

第１のアプリケーションのセキュリティが満足できるか否かを確認するセキュリティ確認工程と、

セキュリティが満足できるときに、セキュリティステータスを、前記セキュアな領域に設定するセキュリティステータス設定工程と、

前記第１のアプリケーションから第２のアプリケーションへの切替時に、前記セキュアな領域に設定されたセキュリティステータスを退避させるセキュリティステータス退避工程と、

暗号を作成し、その作成した暗号を暗号化キーとして保存し、次に、その暗号化キーに基づいて暗号情報を作成して前記ノンセキュアな領域に保存する暗号保存工程と、

前記第２のアプリケーションから前記第１のアプリケーションへの切替時に、再度、前記暗号化キーに基づいて暗号情報を作成し、その作成した暗号情報と、前記ノンセキュアな領域に保存されている暗号情報とを比較する暗号比較工程と、

前記暗号比較工程で比較した暗号情報が一致する場合に、前記退避させたセキュリティステータスを前記セキュアな領域に復号させるセキュリティステータス復号化工程とを備えるマルチアプリケーションＩＣカードの処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数のアプリケーションを切り替えて使用するマルチアプリケーションＩＣカード及びその処理方法に関するものである。

【０００２】

【従来の技術】従来、ＩＣカードは、例えば、信販会社のクレジットカードのように、一企業から発行され、その企業の単一アプリケーションのみ組み込まれ、単一機能のみ果たすものが多かった。そのようなＩＣカードでは、図５に示すように、まず、暗証番号等を照合（ＶＥＲＩＦＹ）し（ステップ（以下「Ｓ」という。）３１０）、セキュリティが満足されていることが確認できたときは、セキュリティステータス（Ｓｅｃｕｒｉｔｙ　Ｓｔａｔｕｓ（ＳＳ））が設定され（Ｓ３２０）、処理コマンド（例えば、ＲＥＡＤ　ＲＥＣＯＲＤ）が実行される（Ｓ３３０）。ところが、最近では、例えば、信販会社のクレジットカード機能と、家電量販店のポイントカード機能というように、複数企業のアプリケーションが１枚のカードに組み込まれた、いわゆるマルチアプリケーションＩＣカードが普及しつつある。このようなＩ

Ｃカードによれば、例えば、家電量販店での買い物に、まず、家電量販店のポイントで支払い、不足分をクレジットカードで支払うことを、１枚のＩＣカードで済ませることができる。

【０００３】

【発明が解決しようとする課題】しかし、クレジットカード兼ポイントカードのようなマルチアプリケーションＩＣカードの場合は、例えば、ポイントカードについてのセキュリティステータス（ＳＳ）に基づいて、クレジットカードの処理が行われたりすることのないように、アプリケーションが切り替わると、前のアプリケーションのセキュリティステータス（ＳＳ）は、リセットされる。そのため、図６に示すように、初めのＶＥＲＩＦＹ（Ｓ４１０）に基づいて、ポイントカードのセキュリティステータス（ＳＳ）が設定されるが（Ｓ４２０）、続いて、クレジットカードのアプリケーションが選択（ＳＥＬＥＣＴ）され（Ｓ４３０）、クレジットカードのセキュリティステータス（ＳＳ）が設定されると、元のポイントカードのセキュリティステータス（ＳＳ）がリセットされるので（Ｓ４４０）、再度、ポイントカードのＲＥＡＤ　ＲＥＣＯＲＤコマンド処理することができず（Ｓ４５０）、エラー（ＥＲＲ）になる（Ｓ４６０）。したがって、このような場合は、ポイント支払い時、クレジット支払い時、クレジット支払いに基づく新たなポイント加算時と、３回、図５に示す処理を繰り返さなければならず、直前に入力した暗証番号を再度入力しなければならない場合があるなど、処理時間が、かかっていた。

【０００４】本発明の課題は、処理時間を短縮することができ、セキュリティ性の高いマルチアプリケーションＩＣカード及びその処理方法を提供することである。

【０００５】

【課題を解決するための手段】本発明は、以下のような解決手段により、前記課題を解決する。なお、理解を容易にするために、本発明の実施形態に対応する符号を付して説明するが、これに限定されるものではない。前記課題を解決するために、請求項１の発明は、切り替えて実行する複数のアプリケーションを有し、アプリケーション切替時に切替前のアプリケーションの情報をリセットして切替後のアプリケーションからはアクセス不能なセキュアな領域（１２ａ）を含む記憶手段（１２）を有するマルチアプリケーションＩＣカードであって、第１のアプリケーションのセキュリティが満足できるか否かを確認するセキュリティ確認手段（１１）と、セキュリティが満足できるときに、セキュリティステータスを、前記セキュアな領域（１２ａ）に設定するセキュリティステータス設定手段（１２）と、前記第１のアプリケーションから第２のアプリケーションへの切替時に、前記セキュアな領域（１２ａ）に設定されたセキュリティステータスを退避させるセキュリティステータス退避手段（１３）と、前記第２のアプリケーションから前記第１のアプリケーションへの切替時に、前記セキュリティステータス退避手段（１３）に退避させられたセキュリティステータスを前記セキュアな領域（１２ａ）に復号させるセキュリティステータス復号化手段（１２）とを備えるマルチアプリケーションＩＣカードである。

【０００６】請求項２の発明は、請求項１に記載のマルチアプリケーションＩＣカードにおいて、前記記憶手段（１２）は、アプリケーション切替後も切替前の記憶を保持し、切替後のアプリケーションからもアクセス可能なノンセキュアな領域（１２ｂ）を含み、前記セキュリティステータス退避手段（１３）に退避させられたセキュリティステータスの復号を許可するための暗号情報を作成して前記ノンセキュアな領域（１２ｂ）に保存する暗号保存手段（１２）と、前記第１のアプリケーションから前記第２のアプリケーションに切り替えた後、再度、前記第１のアプリケーションに切り替えたときに、再度、暗号情報を作成し、その作成した暗号情報と、前記ノンセキュアな領域（１２ｂ）に保存されている暗号情報とを比較する暗号比較手段（１１）とを備え、前記セキュリティステータス復号化手段（１２）は、前記暗号比較手段（１１）で比較した暗号情報が一致する場合に、前記退避させたセキュリティステータスを復号させることを特徴とするマルチアプリケーションＩＣカードである。

【０００７】請求項３の発明は、請求項２に記載のマルチアプリケーションＩＣカードにおいて、前記暗号保存手段（１２）は、初めに、暗号を作成し、その作成した暗号を暗号化キーとして保存し、次に、その暗号化キーに基づいて暗号情報を作成し、前記暗号比較手段（１１）は、前記暗号化キーに基づいて暗号情報を作成することを特徴とするマルチアプリケーションＩＣカードである。

【０００８】請求項４の発明は、切り替えて実行する複数のアプリケーションを有し、アプリケーション切替時に切替前のアプリケーションの情報をリセットして切替後のアプリケーションからはアクセス不能なセキュアな領域（１２ａ）及びアプリケーション切替後も切替前の記憶を保持し、切替後のアプリケーションからもアクセス可能なノンセキュアな領域（１２ｂ）を含む記憶手段（１２）を有するマルチアプリケーションＩＣカードの処理方法であって、第１のアプリケーションのセキュリティが満足できるか否かを確認するセキュリティ確認工程（Ｓ１１０）と、セキュリティが満足できるときに、セキュリティステータスを、前記セキュアな領域（１２ａ）に設定するセキュリティステータス設定工程（Ｓ１２０）と、前記第１のアプリケーションから第２のアプリケーションへの切替時に、前記セキュアな領域（１２ａ）に設定されたセキュリティステータスを退避させるセキュリティステータス退避工程（Ｓ１２２）と、暗号

を作成し、その作成した暗号を暗号化キーとして保存し、次に、その暗号化キーに基づいて暗号情報を作成して前記ノンセキュアな領域（１２ｂ）に保存する暗号保存工程（Ｓ１２５）と、前記第２のアプリケーションから前記第１のアプリケーションへの切替時に、再度、前記暗号化キーに基づいて暗号情報を作成し、その作成した暗号情報と、前記ノンセキュアな領域（１２ｂ）に保存されている暗号情報とを比較する暗号比較工程（Ｓ１６０）と、前記暗号比較工程（Ｓ１６０）で比較した暗号情報が一致する場合に、前記退避させたセキュリティステータスを前記セキュアな領域（１２ａ）に復号させるセキュリティステータス復号化工程（Ｓ１７０）とを備えるマルチアプリケーションＩＣカードの処理方法である。

【０００９】

【発明の実施の形態】以下、図面等を参照して、本発明の実施の形態について、さらに詳しく説明する。図１は、本発明によるマルチアプリケーションＩＣカードの実施形態を示すブロック図である。マルチアプリケーションＩＣカード１０は、制御部１１と、ＲＡＭ１２と、ＥＥＰＲＯＭ１３とを備える。

【００１０】制御部１１は、本マルチアプリケーションＩＣカード１０全体の制御を行う部分である。ＲＡＭ１２は、セキュリティステータス（ＳＳ）等のデータを記憶する揮発性メモリであり、Ｄｙｎａｍｉｃである。ＲＡＭ１２は、セキュアなＲＡＭ領域１２ａと、ノンセキュアなＲＡＭ領域１２ｂとを有する。セキュアなＲＡＭ領域１２ａは、アプリケーションを切り替えると、セキュリティ保持のために切替前の記憶をリセットし、切替後のアプリケーションからはアクセスできない領域である。ノンセキュアなＲＡＭ領域１２ｂは、アプリケーションを切り替えても、切替前の記憶を保持しておき、切替後のアプリケーションや外部からアクセス可能な領域であり、Ｐｕｂｌｉｃである。

【００１１】ＥＥＰＲＯＭ１３は、Ｒａｎｄｏｍ Ｎｕｍｂｅｒ Ｓｅｅｄ、Ｄｕｐｌｉａｔｅｄ ＳＳ、Ｓｔａｔｉｃ Ｓｅｓｓｉｏｎ Ｋｅｙ等のデータを記憶する不揮発性メモリであり、Ｓｔａｔｉｃである。Ｒａｎｄｏｍ Ｎｕｍｂｅｒ Ｓｅｅｄは、乱数を発生させるの際の、いわゆる種となるデータである。Ｒａｎｄｏｍ Ｎｕｍｂｅｒ Ｓｅｅｄは、８バイトのデータであり、初期値は、０００００００００００００００ｈである。Ｄｕｐｌｉａｔｅｄ ＳＳは、セキュリティステータス（ＳＳ）を複製したデータであり、後述のように、セキュリティステータス（ＳＳ）を復元する際の元となるデータである。Ｄｕｐｌｉａｔｅｄ ＳＳは、１バイトのデータであり、初期値は、００ｈである。Ｓｔａｔｉｃ Ｓｅｓｓｉｏｎ Ｋｅｙは、Ｒａｎｄｏｍ Ｎｕｍｂｅｒ Ｓｅｅｄを暗号化する際の鍵となるデータである。Ｓｔａｔｉｃ ＳｅｓｓｉｏｎＫｅｙは、８バイトのデータであり、初期値は、０００００００００００００００ｈである。

【００１２】図２は、本発明の実施形態に係るマルチアプリケーションＩＣカードの動作を説明するフローチャートである。制御部１１の動作を中心として、マルチアプリケーションＩＣカード１０の動作を説明する。制御部１１は、暗証番号等の照合（ＶＥＲＩＦＹ）を行い（Ｓ１１０）、セキュリティが満足できれば、セキュリティステータス（ＳＳ）の設定を行う（Ｓ１２０）。制御部１１は、別のアプリケーションを選択するＳＥＬＥＣＴコマンドを受信して（Ｓ１３０）、そのアプリケーションを実行（ＬＯＡＤ）した後（Ｓ１４０）、再度、元のアプリケーションを選択するＳＥＬＥＣＴコマンドを受信したら（Ｓ１５０）、認証コードチェックを行う（Ｓ１６０）。認証コードが正しいときは、制御部１１は、ＥＥＰＲＯＭ１３に複製しておいたセキュリティステータス（Ｄｕｐｌｉａｔｅｄ ＳＳ）を復号化して（Ｓ１７０）、セキュアなＲＡＭ領域１２ａに書き込み（Ｓ１８０）、ＲＥＡＤ ＲＥＣＯＲＤコマンドを実行する（Ｓ１９０）。一方、認証コードが正しくないときは、制御部１１は、再度、セキュリティが満足できるか否かを照合（ＶＥＲＩＦＹ）し（Ｓ２００）、セキュリティが満足できれば、セキュリティステータス（ＳＳ）の設定を行った後（Ｓ２１０）、ＲＥＡＤ ＲＥＣＯＲＤコマンドを実行する（Ｓ１９０）。

【００１３】図３は、セキュリティステータスの設定動作の詳細について説明するフローチャートである。ＶＥＲＩＦＹの結果、セキュリティが満足できるときは、制御部１１は、セキュアなＲＡＭ領域１２ａにセキュリティステータス（ＳＳ）をセットする（Ｓ１２１）。そして、制御部１１は、そのセットしたセキュリティステータス（ＳＳ）を、ＥＥＰＲＯＭ１３にＤｕｐｌｉａｔｅｄ ＳＳとしてコピーする（Ｓ１２２）。続いて、制御部１１は、乱数を生成して、その生成した乱数をＥＥＰＲＯＭ１３にＲａｎｄｏｍ Ｎｕｍｂｅｒ Ｓｅｅｄとして保存し（Ｓ１２３）、また、このＲａｎｄｏｍ Ｎｕｍｂｅｒ Ｓｅｅｄを、ＥＥＰＲＯＭ１３に予め設定してあるＳｔａｔｉｃ Ｓｅｓｓｉｏｎ Ｋｅｙをキーとして、ＥＣＢ ＤＥＳ暗号化し、暗号化結果を新たなＳｔａｔｉｃ Ｓｅｓｓｉｏｎ ＫｅｙとしてＥＥＰＲＯＭ１３に保存する（Ｓ１２４）。さらに、制御部１１は、Ｒａｎｄｏｍ Ｎｕｍｂｅｒ Ｓｅｅｄを、Ｓ１２４において生成したＳｔａｔｉｃ Ｓｅｓｓｉｏｎ Ｋｅｙをキーとして、再度、ＥＣＢ ＤＥＳ暗号化して、その暗号化結果を、今度は、ノンセキュアなＲＡＭ領域１２ｂのＥｎｃｉｐｈｅｒｅ Ｒａｎｄｏｍ Ｎｕｍｂｅｒとして格納する（Ｓ１２５）。

【００１４】図４は、認証コードチェック動作の詳細について説明するフローチャートである。制御部１１は、ＥＥＰＲＯＭ１３に保存されているＲａｎｄｏｍ Ｎｕ

ｍｂｅｒ　Ｓｅｅｄ及びＳｔａｔｉｃ　Ｓｅｓｓｉｏｎ　Ｋｅｙを読み出し（Ｓ１６１）、Ｓｔａｔｉｃ　Ｓｅｓｓｉｏｎ　Ｋｅｙをキーとして、Ｒａｎｄｏｍ　Ｎｕｍｂｅｒ　Ｓｅｅｄを、ＥＣＢ　ＤＥＳ暗号化して（Ｓ１６２）、その暗号化結果と、ノンセキュアなＲＡＭ領域１２ｂのＥｎｃｉｐｈｅｒｅ　ＲａｎｄｏｍＮｕｍｂｅｒとを比較する（Ｓ１６３）。その結果、両者が同一のときは、図２に示すように、ＥＥＰＲＯＭ１３のＤｕｐｌｉａｔｅｄ　ＳＳを、セキュアなＲＡＭ領域１２ａにセキュリティステータス（ＳＳ）としてコピーして復号化するが（Ｓ１７０）、両者が同一でないときは、復号化せず、再度、ＶＥＲＩＦＹする（Ｓ２００）。

【００１５】本実施形態によれば、一旦、確認したセキュリティステータス（ＳＳ）を保存するので、再度、ＶＥＲＩＦＹする必要がなく、処理速度を短縮化することができる。また、毎回、Ｓｔａｔｉｃ　Ｓｅｓｓｉｏｎ　Ｋｅｙを変更して保存するので、毎回、暗号が変わり、セキュリティ性が高い。

【００１６】（変形形態）以上説明した実施形態に限定されることなく、種々の変形や変更が可能であって、それらも本発明の均等の範囲内である。例えば、暗号化方法としては、ＥＣＢ　ＤＥＳ暗号に限らず、他の公知の方法で暗号化しても、同様の効果が得られる。

【００１７】

【発明の効果】以上詳しく説明したように、請求項１の発明によれば、第１のアプリケーションから第２のアプリケーションへの切替時に、第１のアプリケーションのセキュリティステータスを退避させ、第２のアプリケーションから第１のアプリケーションへの切替時に、その退避させたセキュリティステータスを復号させるので、再度、ＶＥＲＩＦＹする必要がなく、処理速度を短縮化することができる。

【００１８】請求項２の発明によれば、セキュリティステータスの復号を許可するための暗号情報をノンセキュアな領域に保存し、第１のアプリケーションから第２のアプリケーションに切り替えた後、再度、第１のアプリケーションに切り替えたときに、再度、暗号情報を作成して、両暗号を比較して、セキュリティステータスを復号化するので、セキュリティ性が高い。

【００１９】請求項３の発明によれば、暗号化キーを作成して、その暗号化キーに基づいて暗号情報を作成するので、毎回、暗号が変わり、セキュリティ性が高い。

【００２０】請求項４の発明によれば、第１のアプリケーションから第２のアプリケーションへの切替時に、第１のアプリケーションのセキュリティステータスを退避させ、第２のアプリケーションから第１のアプリケーションへの切替時に、暗号に基づいて、その退避させたセキュリティステータスを復号させるので、再度、ＶＥＲＩＦＹする必要がなく、処理速度を短縮化することができるとともに、セキュリティ性が高い。

【図面の簡単な説明】

【図１】本発明によるマルチアプリケーションＩＣカードの実施形態を示すブロック図である。

【図２】本発明の実施形態に係るマルチアプリケーションＩＣカードの動作を説明するフローチャートである。

【図３】セキュリティステータスの設定動作の詳細について説明するフローチャートである。

【図４】認証コードチェック動作の詳細について説明するフローチャートである。

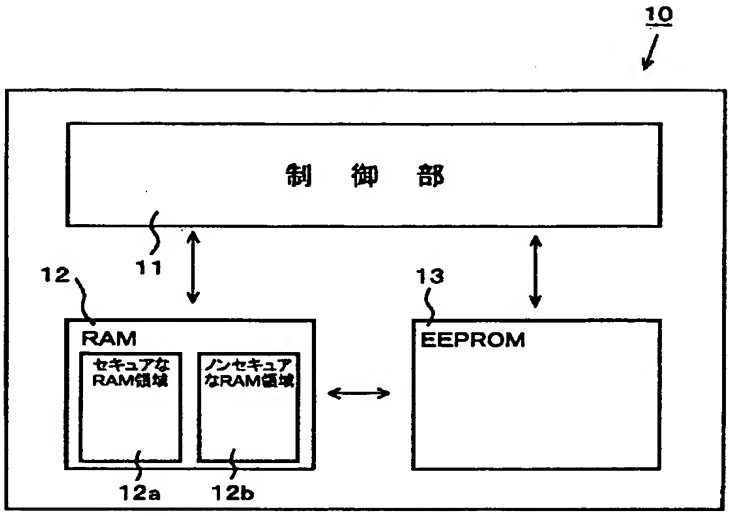
【図５】従来の単一機能ＩＣカードの動作を説明するフローチャートである。

【図６】マルチアプリケーションＩＣカードの動作を説明するフローチャートである。

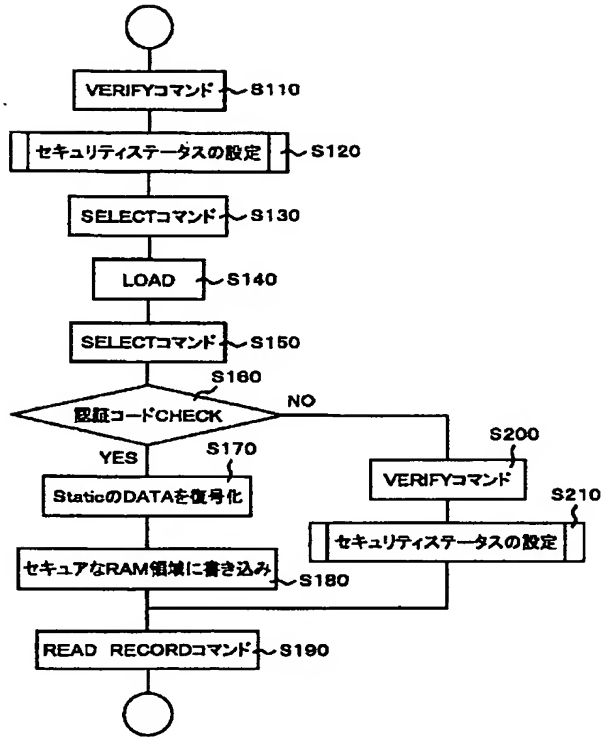
【符号の説明】

１０　マルチアプリケーションＩＣカード
１１　制御部
１２　ＲＡＭ
１２ａ　セキュアなＲＡＭ領域
１２ｂ　ノンセキュアなＲＡＭ領域
１３　ＥＥＰＲＯＭ

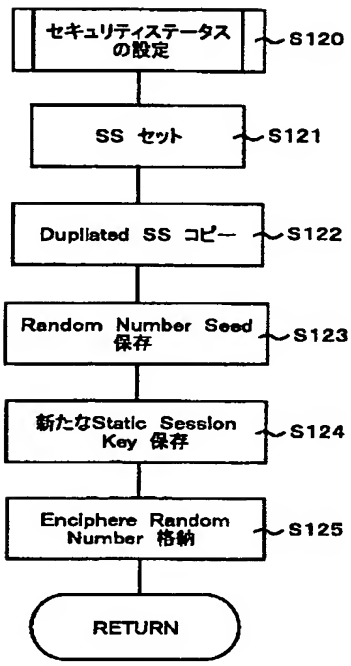
【図１】


10
制　御　部
11
12
13
RAM
セキュアなRAM領域
ノンセキュアなRAM領域
EEPROM
12a
12b

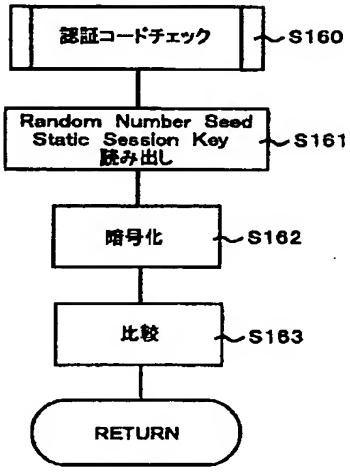
【図２】


VERIFYコマンド
S110
セキュリティステータスの設定
S120
SELECTコマンド
S130
LOAD
S140
SELECTコマンド
S150
S160
認証コードCHECK
NO
YES
S170
StaticのDATAを復号化
S200
VERIFYコマンド
S210
セキュリティステータスの設定
セキュアなRAM領域に書き込み
S180
READ RECORDコマンド
S190

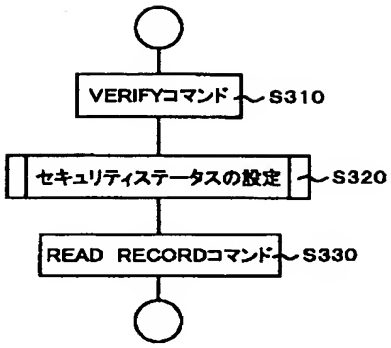
【図３】


セキュリティステータスの設定
S120
SS セット
S121
Duplated SS コピー
S122
Random Number Seed 保存
S123
新たなStatic Session Key 保存
S124
Encipher Random Number 格納
S125
RETURN

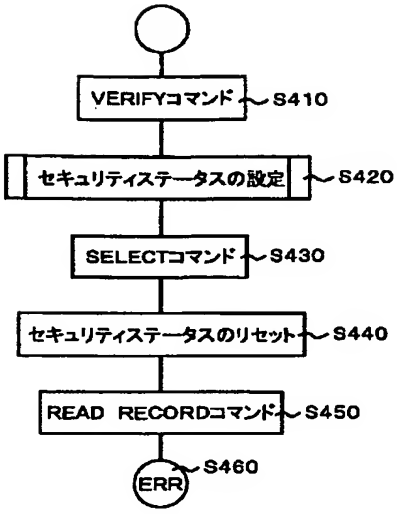
【図４】


認証コードチェック
S160
Random Number Seed Static Session Key 読み出し
S161
暗号化
S162
比較
S163
RETURN

【図５】



【図６】



フロントページの続き

(72)発明者　近田　恭之
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

Ｆターム(参考)　5B017 AA07 BA02 BB09 CA14
5B035 AA06 BB09 BC00 CA39
5B076 AB17 FB01